Seminars

Site: Your Learning Platform
Module: Security and Risk Management October 2024
Book: Seminars
Printed by: Md Chowdhury
Date: Friday, 24 January 2025, 11:11 AM

Description

Seminar materials for Security and Risk Management (SRM_PCOM7E) module.

To print the entire resource or a specific seminar, click on the cog to start.

Table of contents

Unit 1 Seminar

Title: Introductory Seminar

This live session aims to introduce you to the module. It covers the module structure, delivery, and assessments. It is an opportunity for you to also seek clarification on any aspect of module content that may not be clear. This is to ensure you have clearer understanding of what is expected. It also serves as a networking session where tutors and students introduce themselves and get to know each other before the module begins.

There will be a discussion/ briefing on the assessments for this module. As it involves a team project, you will need to read the Group/Teamwork guidance on the **Department homepage** regarding team roles and the scoring of team activities.

Teams will be assigned and there is a deadline at the end of this week for the final group contract to be agreed by each team. A copy will need to be emailed to the module tutor. If you cannot attend this session, please get in touch with the module tutor as soon as possible.

Unit 2 Seminar

Title: User Participation in the Risk Management Process

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Read the Spears & Barki (2010) article then prepare answers to the following questions:

a. How did the authors use both Qualitative and Quantitative assessment approaches? What benefits did each approach yield?
b. What do the authors list as the advantages of involving users in the risk management process?
c. Based on the findings of the research,
    i. How will the lack of user access affect the risk assessment you will carry out as part of your assessment?
    ii. Will it affect the choice of Qualitative vs. Quantitative assessment methods you utilise?
    iii. How might you mitigate any issues encountered?

You should demonstrate that you understand the topic covered and ensure you use references to academic literature (including journals, books, and reports). This activity will provide evidence of your personal growth and is a component of the e-portfolio, which you can submit at the end of the module.

We will review some of your answers in this week's seminar, as well as covering more on the content of Units 1 and 2. There will also be an opportunity to review your team's progress during the seminar.

Unit 4 Seminar

Title: Threat Modelling Exercises

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Read Shostack (2018) chapters 3 – 5 (that cover STRIDE and DREAD, Attack Trees and Attack libraries) as well as Spring et al (2021) (that discusses the history and some failings with CVSS) and then create a threat model based on one of the following scenarios:

1. A large international airport based in the United States of America.
2. A large international bank based in the UK.
3. A large nuclear power station in France.

You should use the Threat modelling Manifesto, the OWASP Threat modelling Cookbook and the ATT&CK libraries to inform your model design. Be prepared to share and discuss your designs at the seminar session this week.

You should also add your individual designs to your e-portfolio.

Unit 6 Seminar

Title: Security Standards

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Review the following links/ websites and answer the questions below:

ICO (2020) **Guide to the General Data Protection Regulation (GDPR).**

PCI Security Standards.org (2020) **Official PCI Security Standards Council Site - PCI Security Standards Overview.**

HIPAA (2020) **HIPAA For Dummies – HIPAA Guide.**

- Which of the standards discussed in the sources above would apply to the organisation discussed in the assessment? For example, a company providing services to anyone living in Europe or a European-based company or public body would most likely be subject to GDPR. A company handling online payments would most likely need to meet PCI-DSS standards.
- Evaluate the company against the appropriate standards and decide how would you check if standards were being met?
- What would your recommendations be to meet those standards?
- What assumptions have you made?

We will be discussing these articles and the wiki in this week's seminar. After the seminar, review your initial response as well as those of your colleagues. There will also be an opportunity to review your team's progress during the seminar.

Unit 8 Seminar

Title: Quantitative Risk Modelling

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Part A

Read Goerlandt et al (2017), Hugo et al (2018) and Çelikbilek & Tüysüz (2020) and answer the following questions:

1. How do Goerlandt et al (2017) suggest that the validity of QRA approaches can be validated? What did they posit was the most effective approach?
2. Which techniques did Hugo et al (2018) should be applied to project management? What were their recommendations to increase the use of QR analysis in Projects?

3. The last paper reviews various Multi-Criteria Decision Methods (MCDMs) and considered the relative accuracy and validity of the techniques. Which did they find was the most accurate of the methods compared? What were the failings of the general TOPSIS approach?

Part B

Read chapter 5 of the course text (Olsen & Desheng (2020) and implement the inventory Monte Carlo simulation. You can use Yasai (Eckstein & Riedmuller, 2002) to replace crystal ball. If you have difficulty implementing the course text model, there is a simplified model also available. Their paper gives instructions on its use. Be prepared to discuss your results in the seminar.

You should add your answers to your e-portfolio and be prepared to discuss them as part of this week's seminar.

Unit 10 Seminar

Title: DR Solutions Design and Review

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Part A

Read Opara-Martins et al (2014) and Morrow et al (2021) and answer the following questions:

1. What are some of the main vendor lock-in issues the authors identify? How would you mitigate them?
2. What are some of the security concerns with the modern cloud? How can these be mitigated?

Part B

Create a high-level diagram of a DR solution for each of the following requirements. They should be created in PowerPoint, and you should include a basic description of each design. **Be prepared to share and discuss your designs in this week's seminar.**

1. RPO= 1 hr; RTO= 8 hrs; high availability (HA) required.
2. RPO= 24 hrs; RTO = 72 hrs; HA NOT required.
3. RPO= 5 mins; RTO= 1 hr; HA required.

Add your answers to your e-portfolio and be prepared to discuss them at the seminar this week.

Unit 12 Seminar

Title: The Great Debate - The Future of SRM

Each team will choose a trend that they think will be the most influential in the next 5 years and will prepare a 10-minute presentation on that trend that summaries the key points and argues why they believe it will be the most influential in the next 5 years. Each team will be given a slot in this week's seminar where they will be able to present their slides and their arguments. Following the presentations, all attendees will be given a chance to ask questions and discuss their own views. At the end of the discussion the tutor will run a poll and all attendees will be given the chance to vote for their favourite.

Learning Outcomes

- Identify and analyse critically, security risks, threats and vulnerabilities in information systems, accounting for the current threat landscape
- Gather and synthesise information from multiple sources (including internet security alerts & warning sites) to aid in the systematic analysis of risks & security issues

- Critically determine appropriate methodologies, tools and techniques to mitigate and/or solve security risks and their business impact
- Articulate the legal, social, ethical, and professional issues faced by information security and risk professionals